Ray, Kathy (OST)

From:	O'Berry, Donna (OST)
Sent:	Thursday, October 13, 2011 5:26 AM
To:	Hopkins, Lawrence (OST); Orndorff, Andrew (OST); Ellis, Sherri (OST); Stubblefield, Angela H <FAA>; Brandon, Skip <FAA>; Charles, Frederic K <FAA>; Widawski, Lou (OST); Szakal, Keith (OST); Slaughter, Stephen CTR (OST); Price, Donald (OST)
Cc:	Lowder, Michael (OST); Lee, Rob (OST); Stovall, Amy (OST); Renfro, Donna (OST); Dipietra, Paul (OST); Toney, Michael (OST); Gary.Golas; Golas, Gary (OST); ford, Mark (OST); Barrett, Claire (OST)
Subject:	RE: WikiLeaks Executive Order Published Today
Attachments:	EO 13587.pdf

Official version – EO number is 13587.

From: Hopkins, Lawrence (OST)
Sent: Friday, October 07, 2011 11:26 AM
To: Orndorff, Andrew (OST); Ellis, Sherri (OST); O'Berry, Donna (OST); Stubblefield, Angela H <FAA>; Brandon, Skip <FAA>; Charles, Frederic K <FAA>; Widawski, Lou (OST); Szakal, Keith (OST); Slaughter, Stephen CTR (OST); Price, Donald (OST)
Cc: Lowder, Michael (OST); Lee, Rob (OST); Stovall, Amy (OST); Renfro, Donna (OST); Dipietra, Paul (OST); Toney, Michael (OST); Gary.Golas; Golas, Gary (OST); ford, Mark (OST); Barrett, Claire (OST)
Subject: WikiLeaks Executive Order Published Today

Good Morning All,

I just received the WikiLeaks EO from the PM-ISE. Please review at your convenience.

Lawrence V. Hopkins
Associate Director for Intelligence
Office of Intelligence, Security and Emergency Response (S-60)
Office of the Secretary
United States Department of Transportation
202-366-6528

Presidential Documents

Executive Order 13587 of October 7, 2011

Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

Section 1. *Policy.* Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

Sec. 2. *General Responsibilities of Agencies.*

Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and

(e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

Sec. 3. *Senior Information Sharing and Safeguarding Steering Committee.*

Sec. 3.1. There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

Sec. 3.2. The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

Sec. 3.3. The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;

(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch's successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government-wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager-Information Sharing Environment (PM–ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PPD–1 of February 13, 2009 (Organization of the National Security Council System).

Sec. 4. *Classified Information Sharing and Safeguarding Office.*

Sec. 4.1. There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM–ISE to provide expert, full-time, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailees, as needed and appropriate, from agencies represented on the Steering Committee.

Sec. 4.2. The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an effective program to monitor compliance with established policies

and standards needed to achieve classified information sharing and safeguarding goals; and

(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

Sec. 5. *Executive Agent for Safeguarding Classified Information on Computer Networks.*

Sec. 5.1. The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the "Executive Agent"), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD–42 of July 5, 1990, as supplemented by and subject to this order.

Sec. 5.2. The Executive Agent's responsibilities, in addition to those specified by NSD–42, shall include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as re-designated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent's timely development and issuance of technical policies and standards;

(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

Sec. 6. *Insider Threat Task Force.*

Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

Sec. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

Sec. 6.3. The Task Force's responsibilities shall include the following:

(a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;

(e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

Sec. 7. *General Provisions.* (a) For the purposes of this order, the word "agencies" shall have the meaning set forth in section 6.1(b) of Executive Order 13526 of December 29, 2009.

(b) Nothing in this order shall be construed to change the requirements of Executive Orders 12333 of December 4, 1981, 12829 of January 6, 1993, 12968 of August 2, 1995, 13388 of October 25, 2005, 13467 of June 30, 2008, 13526 of December 29, 2009, 13549 of August 18, 2010, and their successor orders and directives.

(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12829, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM–ISE under Executive Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD–42 and Executive Order 13286, as amended; the National Counterintelligence Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD–42, and Executive Orders 12333, as amended, 12968, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided herein.

(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower

Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

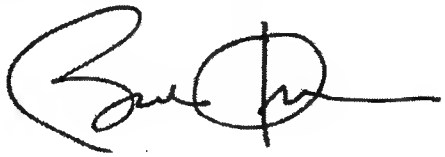
(g) Nothing in this order shall be construed to impair or otherwise affect:

(1) the authority granted by law to an agency, or the head thereof; or

(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



THE WHITE HOUSE,
October 7, 2011.

[FR Doc. 2011–26729
Filed 10–12–11; 11:15 am]
Billing code 3295–F2–P

Ray, Kathy (OST)

From: American Forces Press Service <afps@subscriptions.dod.mil>
Sent: Friday, October 07, 2011 1:12 PM
To: O'Berry, Donna (OST)
Subject: Obama Announces New Classified Information Safeguards

You are subscribed to American Forces News Articles for U.S. Department of Defense. This information has recently been updated, and is now available.

Obama Announces New Classified Information Safeguards

10/07/2011 12:49 PM CDT

Obama Announces New Classified Information Safeguards

By Donna Miles
American Forces Press Service

WASHINGTON, Oct. 7, 2011 - President Barack Obama issued an executive order today that strengthens the government's information and computer security policies and practices to prevent breaches such as the 2010 WikiLeaks episode.

The order follows an interagency committee review of existing policies and practices following WikiLeaks' unlawful disclosure of classified information last summer, White House officials said.

The WikiLeaks.org group posted more than 90,000 documents, many of which detailed classified and sensitive field reports regarding military operations.

Obama's executive order cites efforts already taken to reduce the risk of future security breaches while providing a framework for enhancing national security through responsible sharing and safeguarding of classified information.

"The strategic imperative of our efforts has been to ensure that we provide adequate protections to our classified information while at the same time sharing the information with all who reasonably need it to do their jobs," officials said.

The emphasis, they explained, is on balancing the requirements of responsible information sharing with safeguarding imperatives, while ensuring consistency across government and respecting the American people's privacy, civil rights and civil liberties.

The executive order assigns agencies the primary responsibility for sharing and safeguarding classified information, consistent with appropriate protections for privacy and civil liberties.

Federal agencies that use classified networks are required to:

-- Designate a senior official to oversee the agency's classified information sharing and safeguarding;

-- Implement a program to detect and prevent insider threats; and

-- Conduct self-assessments of policy and standard compliance.

The executive order establishes several new bodies to develop, oversee and enforce these new security reforms.

A senior information sharing and safeguarding steering committee formally established today will coordinate interagency efforts and ensure that the federal departments and agencies are held accountable. In addition, a new classified information sharing and safeguarding office will provide a sustained, full-time focus on sharing and safeguarding classified national security information. The office also will help to ensure consistent policies and standards and strive to identify the next potential problem.

Meanwhile, senior representatives both at the Defense Department and National Security Agency will act together as the executive agent for safeguarding classified information on computer networks. As part of this joint mission, they will develop technical safeguarding polices and standards and assess compliance.

Also, Attorney General Eric H. Holder Jr. and Director of National Intelligence James R. Clapper Jr. are forming a task force to develop a program to detect and prevent insider threats and reduce potential vulnerabilities throughout the government that will integrate specialized abilities, tools and techniques to deter, detect and disrupt the insider threat, officials said.

White House officials noted measures already taken within the Defense Department and other federal agencies to safeguard classified information and networks.

All have made significant progress in clarifying and standardizing polices, processes and technical controls regarding removable media, officials said, limiting the numbers of users with removable media permissions and strengthening accountability for violations.

In addition, owners and operators of classified systems continue to strengthen verification procedures to log on to classified systems and the tracking of what information users access, officials added, noting that more robust access control systems are being implemented to ensure individual users' information access is commensurate with their assigned roles.

Meanwhile, high priority is being placed on enhancing the auditing capabilities across U.S. government classified networks. Planning is now under way to define policy and develop standards for collecting and sharing of audit and insider threat data, officials said.

Douglas B. Wilson, assistant secretary of defense for public affairs, noted this spring that the WikiLeaks episode underscores the need for laws and policies that address the unintended consequences of "technology at the intersection of national security."

"Classified information is classified information, and releasing that information is illegal," Wilson said during an April 17 interview with Vago Muradian on "This Week in Defense News."

"But I think that we have a lot to do in government to understand that we need to be focusing much more on policy and much more on the laws that we need to think about to address what have been very unintended consequences of technological advance," he said.

Even as social media revolutionizes information-sharing, the Defense Department's communication strategy boils down to the responsibility of being transparent and timely without jeopardizing the safety and privacy

of service members and their families, Wilson said.

"How do you deal with the press and public openly, credibly, in a timely manner and honestly?" Wilson asked. "How do you provide facts and the truth, by the same token understanding that we're responsible for our men and women in uniform who are in harm's way in many places? How do you make sure that there [are] not unintended consequences of information which can put them further in harm's way and affect their safety and the privacy of their families?

"Those are the issues that frame everything that we do," Wilson said.
ï¿½
Biographies:
Douglas B. Wilson

Ray, Kathy (OST)

Subject:	WikiLeaks Update - Decisions Made at Recent Deputies Committee Meeting
Location:	5 Floor SCIF (W54-120)
Start:	Wed 6/15/2011 10:00 AM
End:	Wed 6/15/2011 11:00 AM
Show Time As:	Tentative
Recurrence:	(none)
Meeting Status:	Not yet responded
Organizer:	Hopkins, Lawrence (OST)
Required Attendees:	O'Berry, Donna (OST); Orndorff, Andrew (OST); Ellis, Sherri (OST); Szakal, Keith (OST); Rose, Margaret (OST); Mancuso, Robert; Meade, David (OST); Price, Donald (OST); Dipietra, Paul (OST); Toney, Michael (OST); Stovall, Amy (OST); Sachs, Tom (OST); Benini, Janet (OST); Golas, Gary (OST); Gary.Golas; Slaughter, Stephen CTR (OST); ford, Mark (OST); Renfro, Donna (OST); Stuckey, William (OST)

When: Wednesday, June 15, 2011 10:00 AM-11:00 AM (GMT-05:00) Eastern Time (US & Canada).
Where: 5 Floor SCIF (W54-120)

Note: The GMT offset above does not reflect daylight saving time adjustments.

~~*~*~*~*~*~*~*~*~*~*

Good Afternoon All,

I'd like to invite you to this meeting for the express purpose of bringing you up to date on what the deputies decided regarding actions to be taken – across the government – resultant of WikiLeaks. There is a lot coming down the pike to include new entities that will stand up in the next 90 days to continue to address information sharing and protection of our classified information. I know that I can present all that I need to in less than an hour and have time for questions if you have any. Hope to see everyone there.

Lawrence V. Hopkins
Associate Director for Intelligence
Office of Intelligence, Security and Emergency Response (S-60)
Office of the Secretary
United States Department of Transportation
202-366-6528

Ray, Kathy (OST)

From: O'Berry, Donna (OST)
Sent: Wednesday, January 05, 2011 4:52 PM
To: Harris, Joan (OST)
Subject: RE: REMINDER: 3:30PM today

Thanks, Joan. Please do include me on the IPC email distribution group. Thank you.

From: Harris, Joan (OST)
Sent: Wednesday, January 05, 2011 4:23 PM
To: O'Berry, Donna (OST)
Subject: RE: REMINDER: 3:30PM today

So sorry Donna. Today is my first day back from leave and I guess my brain is still in another time zone (just arrived back to DC about 11PM last night from CA. and when I got up for work today my body still felt like it was 3:30AM.)

Here is a short summary. The whole thing only took about 20 minutes, including introductions.

Attendees: Rob, me, Lou Widawski, Margaret Rose, Sherri Ellis, Tim Gaither, Don Price

Several activities already underway with regard to Wikileaks and the OMB Nov 28 directive to Depts/ Agencies. Purpose today is to make sure those of us around the table with responsibility for one or more of these pieces are aware of the other related actions.

- M40 (Margaret Rose/Rich Thompson) are the leads for the internal DOT security assessment team that was directed by the OMB Nov 28 memo. They have set up this team – with FAA and MARAD reps included – and have held a couple of meetings as they gather info and prepare to respond to OMB by the Jan. 28 deadline.
- S60/Intel (Larry Hopkins) is the DOT lead to the newly established Wikileaks IPC. Per Dec 1 memo from NSS, NSS has appointed Russ Travers to head up the new effort, including the new IPC. I will create a distribution group for incoming and outgoing emails with NSS for the new IPC. The email group will include folks from the offices represented today. *Shall I put you on this email group too?*
- S80 has also been attending NSS meetings on cyber security as part of the regular Cyber and Communications Infrastructure IPC. No one was sure how the NSS intends to coordinate the two parallel IPCs, but clearly M80 has an ongoing interest since this is all about cyber-related issues.
- The CMC has an interest because of the systems they use.

Donna, let me know if you have any questions.

Joan
6-1827

From: O'Berry, Donna (OST)
Sent: Wednesday, January 05, 2011 3:43 PM

To: Harris, Joan (OST)
Subject: RE: REMINDER: 3:30PM today

Joan – are you still planning to call me?

From: Harris, Joan (OST)
Sent: Wednesday, January 05, 2011 11:38 AM
To: O'Berry, Donna (OST)
Subject: RE: REMINDER: 3:30PM today

Great. We'll call you then.

Joan

From: O'Berry, Donna (OST)
Sent: Wednesday, January 05, 2011 11:37 AM
To: Harris, Joan (OST)
Subject: RE: REMINDER: 3:30PM today

EX. 6

Yes [redacted] Thanks!

From: Harris, Joan (OST)
Sent: Wednesday, January 05, 2011 11:34 AM
To: O'Berry, Donna (OST)
Subject: RE: REMINDER: 3:30PM today

Donna – It might be easier if we call you since I don't know the number in that room. Is there a number we can reach you at?

Joan

From: O'Berry, Donna (OST)
Sent: Wednesday, January 05, 2011 11:31 AM
To: Harris, Joan (OST); Hopkins, Lawrence (OST); Rose, Margaret (OST); Ellis, Sherri (OST); Orndorff, Andrew (OST); Thompson, Richard (OST); Price, Donald (OST)
Subject: RE: REMINDER: 3:30PM today

I need to call in. Is there a number? Thanks.

From: Harris, Joan (OST)
Sent: Wednesday, January 05, 2011 11:29 AM
To: Hopkins, Lawrence (OST); Rose, Margaret (OST); Ellis, Sherri (OST); Orndorff, Andrew (OST); Thompson, Richard (OST); Price, Donald (OST); O'Berry, Donna (OST)
Cc: Benini, Janet (OST); Lee, Rob (OST); Widawski, Lou (OST)
Subject: REMINDER: 3:30PM today

Good Morning:

Just a reminder that we will be meeting at 3:30 today to go over coordination for the new Wikileaks IPC and related activities.

See you then.

Joan

From: Harris, Joan (OST)
Sent: Wednesday, December 22, 2010 5:26 PM
To: Hopkins, Lawrence (OST); Rose, Margaret (OST); Ellis, Sherri (OST); Orndorff, Andrew (OST); Thompson, Richard (OST); Price, Donald (OST); O'Berry, Donna (OST)
Cc: Benini, Janet (OST); Lee, Rob (OST); Widawski, Lou (OST)
Subject: LOCATION: coordination for new Wikileaks IPC

All: we will be meeting in **W56-102** at 3:30PM on Wed January 5.

See you then.

Joan

-----Original Appointment-----
From: Harris, Joan (OST)
Sent: Wednesday, December 22, 2010 1:29 PM
To: Hopkins, Lawrence (OST); Rose, Margaret (OST); Ellis, Sherri (OST); Orndorff, Andrew (OST); Thompson, Richard (OST); Price, Donald (OST); O'Berry, Donna (OST)
Cc: Benini, Janet (OST); Lee, Rob (OST); Widawski, Lou (OST)
Subject: coordination for new Wikileaks IPC
When: Wednesday, January 05, 2011 3:30 PM-4:00 PM (GMT-05:00) Eastern Time (US & Canada).
Where: location TBD

You are invited to a quick get together to coordinate DOT participation in the new Wikileaks IPC recently established at NSS. I will let you know the meeting location once I get that confirmed.

Please let me know if you can make this.

Thanks, Joan Harris
6-1827

Ray, Kathy (OST)

From: Thompson, Richard (OST)
Sent: Thursday, December 16, 2010 8:36 AM
To: Meade, David (OST); Rose, Margaret (OST); Jacob, John (OST); Ross, Bob (OST); O'Berry, Donna (OST); Hopkins, Lawrence (OST); Riddle, Mark <FAA>; Shifflett, Jeremy <FAA>; Knieff, Barbara <FAA>; Evancho, Joseph <FAA>; Ellis, Sherri (OST)
Subject: News Article -- Viewing Classified Information on Home Computers

FYI, from Nextgov.com.

Rich

Federal guidance on WikiLeaks raises legal questions

By Brian Kalish 12/14/10

The government might not have the right to restrict federal employees and contractors from viewing on their personal home computers the classified material that WikiLeaks posted, said Kathleen Clark, a law professor at Washington University in St. Louis School of Law with expertise in whistleblower protections and national security.

On Dec. 3, OMB's general counsel office sent a notice to agency general counsels instructing them to remind employees they should not view materials that WikiLeaks posted because the information remains classified.

The memo said federal employees and contractors "shall not . . . access documents that are marked classified," on computers that access nonclassified government systems, including employees' or contractors' personally owned computers.

Clark said the guidance is unclear as to whether employees could access the leaked documents on a personal computer that does not access government systems. OMB did not return a call or e-mail seeking clarification.

"It seems to be fear-mongering," Clark said. The notion that agencies would tell employees they could not view the documents on their home computers "is inexplicable to me," she said.

"I don't think there's any legal authority to assert employees who have security clearances cannot access particular information through their home computers," Clark said.

Both the Defense and State departments told employees and contractors not to access the information, but neither made a distinction between personal and private computers.

Defense's guidance says U.S. military, civilian and contractor employees "should not access the WikiLeaks website to view or download publicized classified information," according to Maj. Chris Perrine, a Defense Department spokesman. Doing so could introduce classified information on unclassified networks, creating "spillage," which is costly to clean up, Perrine said.

Ray, Kathy (OST)

From: Thompson, Richard (OST)
Sent: Thursday, December 16, 2010 7:59 AM
To: Rose, Margaret (OST); Meade, David (OST); Ross, Bob (OST); Hopkins, Lawrence (OST); O'Berry, Donna (OST); Price, Donald (OST); Orndorff, Andrew (OST); Ellis, Sherri (OST); Riddle, Mark <FAA>; Shifflett, Jeremy <FAA>
Subject: News Article -- WikiLeaks - Blocking Media Sites

FYI.

Rich

Air Force blocks media sites that post WikiLeaks

(AP) –WASHINGTON (AP) — The Air Force is blocking computer access to The New York Times and other media sites that published sensitive diplomatic documents released by the Internet site WikiLeaks, a spokeswoman said Tuesday.

Air Force Maj. Toni Tones said more than 25 websites have been blocked and cannot be viewed by any Air Force computer. The ban — aimed at preventing the viewing of classified information — does not apply to personal computers.

She said the action was taken by the 24th Air Force, which is commanded by Maj. Gen. Richard Webber and is responsible for cyberwarfare and computer security for the service. The move was approved by Air Force lawyers, she said.

The Army and Navy say they have not taken similar actions.

"If a site has republished the documents, then we block it," she said, adding that the move to prevent access to the media sites was done recently. She said she was not sure of the date.

Tones said the New York Times is the only major U.S. newspaper included in the ban. Others include Der Spiegel in Germany, the Guardian in Britain and Le Monde in France.

Tones said that the 24th Air Force routinely blocks network access to websites that host inappropriate material, including classified information such as that released by WikiLeaks. Any computer on the Air Force network is now unable to link to the sites.

WikiLeaks released more than a quarter million sensitive State Department cables in late November.

The White House on Dec. 3 formally reminded all federal employees and government contractors that anyone without a security clearance is not permitted to read classified documents, such as the diplomatic messages published by WikiLeaks, even on a personal computer at home outside work hours.

It was not immediately clear how the U.S. government would enforce this, but the White House said employees who inadvertently viewed the information should contact their U.S. security offices at work. The notice by the White House Office of Management and Budget said publication of the files by WikiLeaks "has resulted in damage to our national security."

The New York Times Co. issued a statement in response to the action Tuesday, saying "it is unfortunate that the U.S. Air Force has chosen not to allow its personnel access to information that virtually everyone else in the world can access."

Ray, Kathy (OST)

From: Thompson, Richard (OST)
Sent: Monday, December 13, 2010 9:40 AM
To: O'Berry, Donna (OST)
Subject: RE: FOR YOUR IMMEDIATE ATTENTION AND PROMPT ACTION: WikiLeaks: Model Agency Notice to Employees

Donna:

Thank you.

Rich

From: O'Berry, Donna (OST)
Sent: Monday, December 13, 2010 9:31 AM
To: Thompson, Richard (OST)
Subject: FW: FOR YOUR IMMEDIATE ATTENTION AND PROMPT ACTION: WikiLeaks: Model Agency Notice to Employees

Rich – as requested. I will bring a copy as well.

From: OMB General Counsel's Office [mailto:agency-gcs@messages.whitehouse.gov]
Sent: Friday, December 03, 2010 12:21 PM
To: Rivkin, Robert (OST)
Subject: FOR YOUR IMMEDIATE ATTENTION AND PROMPT ACTION: WikiLeaks: Model Agency Notice to Employees

TO: AGENCY GENERAL COUNSELS

The recent disclosure of U.S. Government documents by WikiLeaks has resulted in damage to our national security. Federal agencies collectively, and each federal employee and contractor individually, are obligated to protect classified information pursuant to all applicable laws, as well as to protect the integrity of government information technology systems. It is a function of agency leadership to establish a vigilant climate that underscores the critical importance of the existing prohibitions, restrictions, and requirements regarding the safeguarding of classified information.

Accordingly, agencies are requested immediately to send a notice to all agency employees and contractors reminding them of their obligations to safeguard classified information. A model notice, for use or adaptation by each agency, is attached to this memorandum. Agencies are responsible for communicating this notice promptly to their employees and contractors. If an agency has a legitimate need for personnel to access classified information on publicly available websites, the agency head shall ensure that such access is managed in a manner that minimizes risk to government information technology systems and adheres to established requirements.

Thank you for your cooperation and assistance.

Attachment (Model Agency Notice)

Preeta D. Bansal
OMB General Counsel and Senior Policy Advisor
395-5044

- WikiLeaks_Model_Employee_Notice_120310.docx

Ray, Kathy (OST)

From: Thompson, Richard (OST)
Sent: Monday, December 13, 2010 9:28 AM
To: O'Berry, Donna (OST)
Subject: OMB Memo

Importance: High

Donna:

For reference at this morning's meeting of the DOT Assessment Team on safeguarding classified information, can you bring a copy of the actual OMB memo to
General Counsel's offices dated December 3, the one telling agencies to issue a notice about safeguarding classified information? I have the model notice that they sent, but not their actual memo. Or, you can e-mail it to me before the meeting -- I may have it but I can't find it.

Thanks.

Rich

Ray, Kathy (OST)

From: Broadcast Messages
Sent: Thursday, December 09, 2010 6:09 PM
Subject: Important Message from the Deputy Secretary Regarding Classified Information

TO: **All U.S. Department of Transportation Employees & Contractors**

FROM: **Deputy Secretary John D. Porcari**

SUBJECT: **Notice to U.S. Department of Transportation Employees and Contractors Concerning Safeguarding of Classified Information and Use of Government Information Technology Systems**

The recent disclosure of U.S. Government documents by WikiLeaks has resulted in damage to our national security. Each U.S. Department of Transportation (DOT) employee and contractor is obligated to protect classified information pursuant to all applicable laws, and to use Government information technology systems in accordance with Agency procedures so that the integrity of such systems is not compromised.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on Web sites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, **classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by federal employees and contractors, until it is declassified by an appropriate U.S. Government authority** (Executive Order 13526, *Classified National Security Information*, (December 29, 2009). Section 1.1.(c) states, "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information").

Therefore, DOT employees and contractors are reminded of the following obligations with respect to the treatment of classified information and the use of non-classified Government information technology systems:

- Except as authorized by the Director, Office of Security (M-40) or other authorized DOT officials and pursuant to DOT policies and procedures, DOT employees and contractors shall not, while using computers or other devices (such as Blackberries or Smart Phones) that access the Web on non-classified Government systems, access documents that are marked classified (including classified documents publicly available on WikiLeaks and other Web sites), as doing so risks that material still classified will be placed onto non-classified systems. This requirement applies to access that occurs either through Agency or contractor computers, or through employees' or contractors' personally owned computers that access non-classified Government systems. This requirement does not restrict DOT employee or contractor access to non-classified, publicly available news reports (and other non-classified material) that may, in turn, discuss classified material, as distinguished from access to underlying documents that are marked classified (including if the underlying classified documents are available on public Web sites or otherwise in the public domain).

- The DOT employees and contractors shall not access classified material unless a favorable determination of the person's eligibility for access has been made by the Director of M-40 or another

authorized DOT official, the person has signed an approved non-disclosure agreement, the person has a need to know the information, and the person has received contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

- Classified information shall not be removed from official premises or disclosed without proper authorization.

- The DOT employees or contractors who believe they may have inadvertently accessed or downloaded classified or sensitive information on computers that access the Web via non-classified Government systems, or without prior authorization, should contact their information security offices for assistance.

Thank you for your cooperation and for your vigilance in addressing these responsibilities.

Ray, Kathy (OST)

From: Thompson, Richard (OST)
Sent: Friday, December 10, 2010 7:49 AM
To: Lee, Rob (OST); O'Berry, Donna (OST)
Subject: FW: Important Message from the Deputy Secretary Regarding Classified Information

Rob:
Donna:

FYI --

The S-2 message just came through as a broadcast message to FAA. I was checking to make sure that they got it because we've found in the past that the different operating administrations have their own procedures for distributing messages from OST that are sent to all DOT employees. Sometimes they don't get distributed as they should, so this is good news.

Rich

From: barbara.knieff@faa.gov [mailto:barbara.knieff@faa.gov]
Sent: Friday, December 10, 2010 7:25 AM
To: Joseph.Evancho@faa.gov; Thompson, Richard (OST); Mark.Riddle@faa.gov
Cc: barbara.knieff@faa.gov
Subject: Re: Important Message from the Deputy Secretary Regarding Classified Information

Rich,

It just came thru as a broadcast to FAA.

From: Joseph Evancho
Sent: 12/10/2010 07:22 AM EST
To: "Richard Thompson" <Richard.Thompson@dot.gov>; Barbara Knieff; Mark Riddle
Subject: Re: Important Message from the Deputy Secretary Regarding Classified Information

Rich,

I'm out today. Mark is acting for Barbara and me.

We had not received the memo and are checking to see if there was an IT/email anomaly or other reason.

Joe

From: [Richard.Thompson@dot.gov]
Sent: 12/10/2010 07:12 AM EST
To: Barbara Knieff; Joseph Evancho; Mark Riddle
Subject: FW: Important Message from the Deputy Secretary Regarding Classified Information

Barbara:
Joe:
Mark:

Did this message get through to FAA? Did all of you receive it as a broadcast message from the Deputy Secretary?

Rich

From: Broadcast Messages
Sent: Thursday, December 09, 2010 6:09 PM
Subject: Important Message from the Deputy Secretary Regarding Classified Information

TO: **All U.S. Department of Transportation Employees & Contractors**

FROM: **Deputy Secretary John D. Porcari**

SUBJECT: **Notice to U.S. Department of Transportation Employees and Contractors Concerning Safeguarding of Classified Information and Use of Government Information Technology Systems**

The recent disclosure of U.S. Government documents by WikiLeaks has resulted in damage to our national security. Each U.S. Department of Transportation (DOT) employee and contractor is obligated to protect classified information pursuant to all applicable laws, and to use Government information technology systems in accordance with Agency procedures so that the integrity of such systems is not compromised.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on Web sites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, **classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by federal employees and contractors, until it is declassified by an appropriate U.S. Government authority** (Executive Order 13526, *Classified National Security Information*, (December 29, 2009). Section 1.1.(c) states, "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information").

Therefore, DOT employees and contractors are reminded of the following obligations with respect to the treatment of classified information and the use of non-classified Government information technology systems:

- Except as authorized by the Director, Office of Security (M-40) or other authorized DOT officials and pursuant to DOT policies and procedures, DOT employees and contractors shall not, while using computers or other devices (such as Blackberries or Smart Phones) that access the Web on non-classified Government systems, access documents that are marked classified (including classified

documents publicly available on WikiLeaks and other Web sites), as doing so risks that material still classified will be placed onto non-classified systems. This requirement applies to access that occurs either through Agency or contractor computers, or through employees' or contractors' personally owned computers that access non-classified Government systems. This requirement does not restrict DOT employee or contractor access to non-classified, publicly available news reports (and other non-classified material) that may, in turn, discuss classified material, as distinguished from access to underlying documents that are marked classified (including if the underlying classified documents are available on public Web sites or otherwise in the public domain).

- The DOT employees and contractors shall not access classified material unless a favorable determination of the person's eligibility for access has been made by the Director of M-40 or another authorized DOT official, the person has signed an approved non-disclosure agreement, the person has a need to know the information, and the person has received contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

- Classified information shall not be removed from official premises or disclosed without proper authorization.

- The DOT employees or contractors who believe they may have inadvertently accessed or downloaded classified or sensitive information on computers that access the Web via non-classified Government systems, or without prior authorization, should contact their information security offices for assistance.

Thank you for your cooperation and for your vigilance in addressing these responsibilities.